UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/468,948	12/22/1999	HIROYUKI KURUMATANI	500.38035X00	4306

7590 06/03/2004

ANTONELLI TERRY STOUT & KRAUS
1300 NORTH SEVENTEENTH STREET
SUITE 1800
ARLINGTON, VA 22209

EXAMINER	
MEISLAHN, DOUGLAS J	

ART UNIT	PAPER NUMBER
2137	8

DATE MAILED: 06/03/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)
	09/468,948	KURUMATANI, HIROYUKI
	Examiner	Art Unit
	Douglas J. Meislahn	2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *23 March 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *2,3,6,8 and 9* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *2,3,6,8 and 9* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *23 March 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. This action is in response to the amendment filed 23 March 2004 that cancelled claims 1, 4, 5, 7, and 10-12 while amending the specification and claims 2, 3, 6, 8, and 9. A drawing correction was also submitted.

Response to Arguments

2. Applicant's arguments filed 23 March 2004 have been fully considered but they are not persuasive. Vanstone et al. present a random number k, which is necessarily generated (see element 24 of figure 2). F_q is a field of characteristic 2. See lines 40-53 of page 8 for mention of transforming [kx0, k] to [x_1, z_1]. Agnew et al. show a random number k in, among other places, the second column of page 806. The field F is of characteristic 2, as indicated by its 2^dth power. See the first column of page 808 for mention of transforming [kx0, k] to [x_1, z_1].

3. Applicant's amendments have not overcome the 101 or 112 rejections. Cast in this murky environment, applicant's comments as to the validity of the 103 rejections, while enlightening, are not persuasive.

Claim Rejections - 35 USC § 112

1. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

2. Claims 1-5 and 7-12 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

3. Claims 2, 3, 8, and 9 recite the limitations "said inputted coordinate component x1" in their second clauses, "said coordinate component x2" in the fourth clauses, "said projective coordinate [X_2, Z_2]" in the fifth clauses, "said coordinate component x4" in the sixth clauses, "said projective coordinate [X_4, Z_4]" in the seventh clauses, "said stored projective coordinates [X_1, Z_1], [X_2, Z_2] and [X_4, Z_4]" in the eighth clauses, and "said coordinate component x3" in the ninth clauses. There is insufficient antecedent basis for these limitations in the claims. In all cases, deleting "said" would overcome the rejection. The offending recitations of "said" could also be replaced with "the".

4. Claims 2, 3, 8, and 9 recite the limitations "the x-coordinates" in the fourth clauses and "said stored random number k" in the last clauses. There is insufficient antecedent basis for these limitations in the claims. The claims are entirely unclear as to which x-coordinates are transformed. This ambiguity makes impossible a precise comparison of the claims with the prior art. Change "said" to "the".

Claim Rejections - 35 USC § 101

5. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 2, 3, 8, and 9 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. The subject matter of the claims is mathematical manipulations that are not put to an useful purpose. Including a step in which the mathematical manipulations are used in a cryptographic operation would make the claims statutory. To emphasize the distinction, encrypting data is an useful

process and hence statutory; adding numbers, even if the are points on an elliptic curve, is not necessarily beneficial and hence is non-statutory.

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

7. Claim 6 is rejected under 35 U.S.C. 102(a) as being clearly anticipated by Vanstone et al. (EP 0 874 307 A1). See pages 5-8.

8. Claim 6 is rejected under 35 U.S.C. 102(b) as being clearly anticipated by Agnew et al. ("An Implementation of Elliptic Curve Cryptosystems Over F2155"). See pages 804-813.

Claim Rejections - 35 USC § 103

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10. Claims 2, 3, 8, and 9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Vanstone et al. in view of Chudnovsky et al. ("Sequences of Numbers Generated by Addition in Formal Groups and New Primality and Factorization Tests").

Vanstone et al. present a system of improving the speed of elliptic curve cryptography. They do not say that a random number is used to derive projective coordinates according to the equations given in the claims. Chudnovsky et al. present methods for improving the speed of elliptic curves. As detailed above, the scope of these claims is indefinite, but the examiner believes that, were the scope of the claims clearly defined, the teachings of these two references would render the claims obvious.

Conclusion

11. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Douglas J. Meislahn whose telephone number is (703) 305-1338. The examiner can normally be reached on between 9 AM and 6 PM, Monday through Thursday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A. Morse can be reached on (703) 308-4789. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Douglas J. Meislahn
Examiner
Art Unit 2137

DJM